Probability Elicitation for F-B-C NASA Space Missions

Decision Analysis Society of INFORMS
Seattle, Washington
October 27, 1998

Dr. Ralph F. Miles, Jr.

Engineering Principal
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

email: rmiles2@earthlink.net

New NASA Strategic Environment

- F-B-C: Faster, Better, Cheaper.
  - No more "Flagship" projects.
  - Many launches a year.
  - Implementation time: 18 months.
- LCA: Life-Cycle Cost Analysis.
  - Cost before commitment.
  - Proposal development: One week.
- ISE: Intelligent Synthesis Environment.
  - Model-based design.
  - Petaflop (10^{15}) computing capability.

Intelligent Synthesis Environment

- ❑ Need end-to-end product life-cycle simulation.
  - Reduce uncertainty.
  - Use geographically distributed talent.
  - Capture design knowledge early in life-cycle.
  - Convert data into knowledge.
- ❑ Fact: Large percentage of cost committed with only small percentage of knowledge.
- ❑ Problem: How to close gap between design knowledge and cost commitment.

ISE Major Components

- Components.
  1. Dynamical interface between humans and computers.
     - CAVE, Vision, Dome.
     - Entertainment industry far in lead.
     - Rapid transition from data to intelligence.
  2. Infrastructure for distributed collaboration between diverse teams across world.
  3. Tools for rapid synthesis and simulation tools.
  4. Tools to link complete life-cycle simulation in a virtual collaborative environment.
- Hardware requirements.
  - Petaflop (10^{15}) computing.
  - High-Speed Information Corridors.
- Cultural barrier.

Ref: Dan Goldin, "Tools of the Future," NASA, Washington, DC, 31 January 1998.

F-B-C Design Requirements

- Model-Based designs.
  - Experts provide models which are compounded up to mission level.
    - Design and analysis done in real-time.
  - Requires explicit incorporation of uncertainty.
- F-B-C does not permit "Worst-case designs."
  - Risk cannot be designed out of missions.
- Rapid development cycle.
  - Requires extensive expert judgment.
    - Minimize analysis, test time and cost.
- Will require extensive probability elicitation.
  - For all uncertainties.
    - Randomness of nature (Aleatory or IAEA Type A).
    - Specification error (Model uncertainty or IAEA Type B).
    - Completeness (Unknown unknowns).

JPL Experience in Probability Elicitation

- Flagship projects with Environmental Impact Statements.
  - Voyager to Outer Planets (1977).
  - Galileo to Jupiter (1989).
  - Ulysses to Jupiter and over the sun (1991).
  - Cassini to Saturn (1997).
    - » Launch: October 1997.
    - » Earth flyby: August 1999.
    - » Saturn arrival: 2005.
- Faster-Better-Cheaper Projects.
  - Mars Pathfinder (July 4, 1997 landing).
  - Stardust Project.
    - » Launch: 1999.
    - » Comet Wild 2: 2004.
    - » Earth return: 2006.

Two F-B-C Missions.

- Mars Pathfinder.
  - Landed "Sojourner Truth" Rover on Mars July 4, 1997.
  - Risk assessment done to assess feasibility of design.
    - » Entry, descent, and landing of Lander.
- Stardust Project.
  - Launch in 1999.
  - Encounter Comet Wild-2 in 2004.
  - Flyby of Earth in 2006.
  - Release science capsule to land in Utah desert.
  - Risk assessment done to assess feasibility of design.

JPL Implementation of SRI Phases of Elicitation

- Motivating.
  - Purpose.
  - Training.
- Structuring.
  - Done by System Engineer.
- Conditioning.
  - Discussion.
  - Training.
- Encoding.
  - Odds and reference events for extremes, equally likely for median.
- Verifying.
  - Examine and discuss resulting CDF.

Quality of Probability Elicitation

- **Requisite Model.**
  - Everything in the model needed for decisions.
  - Nothing in the model not needed for decisions.
- **Substantive Goodness in elicitation.**
  - Provided by the technology expert.
- **Normative Goodness in elicitation.**
  - Provided by the elicitor.
  - Training for the technology expert.

Requisite Models.

- Three step process.
  1. Project system engineer and risk assessor jointly developed Fault-Tree Model.
  2. Probability elicitation done with engineers cognizant for each critical event.
  3. Results "rationalized" by project engineer.
- Final result is expert opinion of project engineer.
- Fault-Tree modeled in MS Excel.
- Uncertainties in failure of critical events.
  - Modeled as lognormal distributions.
  - CDF's of probabilities of failure.
- Monte-Carlo simulation for mission CDF.

Training Session.

- Not used for Mars Pathfinder EDL.
  - Problems resulted in confusing process with elicitation.
- Subsequently developed for Stardust Mission.
- Used Closing Dow Industrial 30 for same day.
  - Forty-five minute training session.
- Knowledge base.
  - Knowledge of market.
  - 90 days previous data.
- Training session well received.

Dow 30 Industrials Stock Index

- ❑ Consider the Dow 30 Industrials Stock Index as an example of probability assessment.
- ❑ Given the data you are presented with and your prior knowledge, assess where the Dow will be at the end of the day.
- ❑ What are factors that could cause the Dow to be very low?
- ❑ What are factors that could cause the Dow to be very high?

1% Assessment of Dow

- This is called a “Bear Market.”
- This is your most pessimistic assessment. It would be the value of the Dow if nearly all of the uncertainties were resolved unfavorably.
- This 1% assessment corresponds to Dow values for which the end-of-day values would be lower than your prediction only twice a year.
- For what value do you believe the Dow has only one chance in 100 of being lower at the end of the day?
  - Probability (1%) =

Assessment of Dow Probabilities

- For what probability do you believe the Dow has only x% chance of being lower at the end of the day?
  - Probability (1%) =
  - Probability (10%) =
  - Probability (50%) =
  - Probability (90%) =
  - Probability (99%) =

Sources of Knowledge for F-B-C Missions

- Taxonomy for sources of F-B-C NASA space knowledge.
  - Flight experience.
  - Testing.
  - Analysis.
  - Expert judgment.
- Almost all knowledge is a combination of these sources.
- Expert judgment always present.

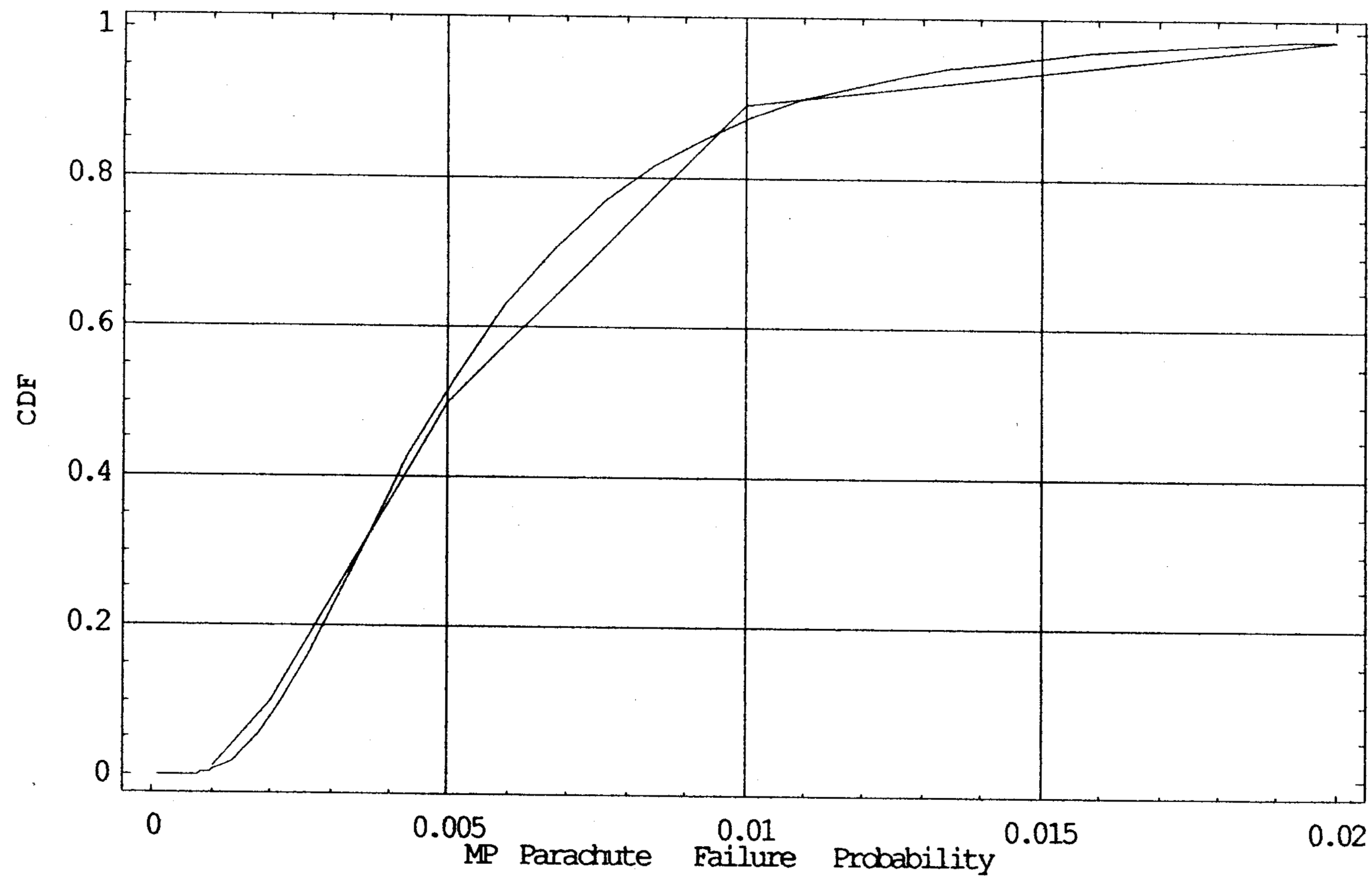
Thinking About Failures

- Three perspectives on failure probabilities.
  1. Think about design, implementation, and operations of similar complexity. How often would this result in failure?
  2. Repeat the design, implementation, and operation for your event many times. How often would this result in failure?
  3. Think of failure events in your life for which statistical evidence exists. Is the failure of your event more or less probable?

Typical Elicitation VG

- ❑ This is your most optimistic assessment. It would be the failure probability if nearly all of the uncertainties were resolved favorably.
- ❑ For what probability do you believe the "true value," if it could be known, has only one chance in 100 of being lower?
  - Probability (1%) =

CDF Plot for Critical Event



Mars Pathfinder Entry, Descent and Landing

- Eight month cruise from Earth to Mars.
- Separate Lander from Cruise Stage (T - 35 min).
- Atmospheric entry with ablative heat-shield (T - 5 min).
- Parachute deploy and heat-shield separation (T - 2 min).
- Radar locks on Mars Surface (T - 25 sec).
- Airbags deploy (T - 5 sec).
- Retro-rockets fire (T - 3 sec).
- Free-fall from 15 meters (T - 1 sec).
- Bounce on surface and roll to stop (1 km).
- Deflate airbags and petal deployment (T + 3 hours).

Mars Pathfinder Risk Assessment

- Entry-Descent-Landing risk assessment.
- All events in series--no redundancy.
- Mission modeled as series elements in MS Excel.
- Monte-Carlo simulation in @RISK.
- Cognizant engineers for each failure event interviewed.
- No training session for probability elicitation.
- Two Deputy Project Engineers independently assessed probability of failure at mission level.
- Results presented at launch-readiness review.
- PRA done too late in development to influence design.
- Did alert Project to areas needing extensive testing.

Mars Pathfinder Fault Tree

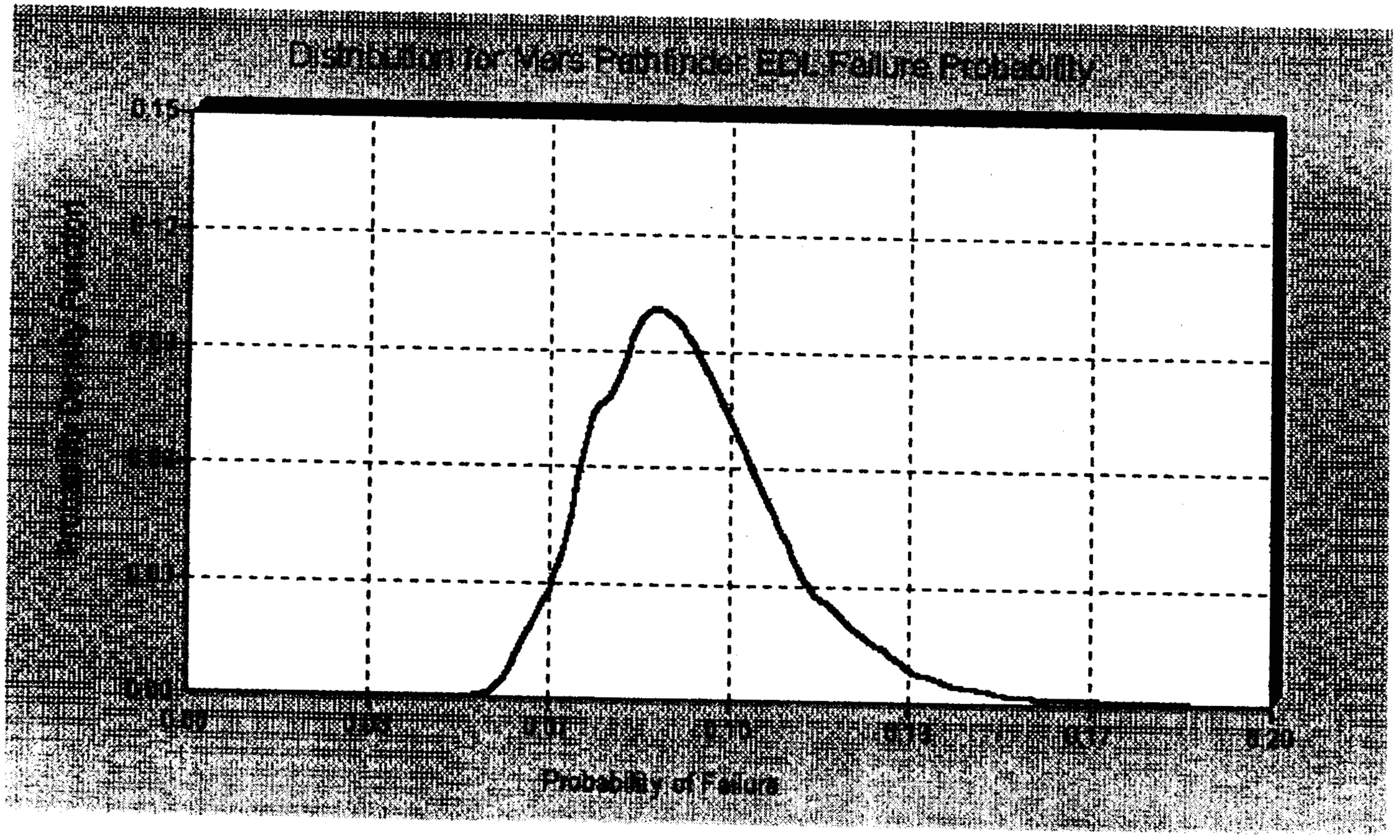
R. Miles **September 12, 1996** **Run SWT960812a.** **Data Set: S. Thurman 8/12/96**

Latin-Hypercube Simulation; 10,000 trials.

Mars Pathfinder EDL Failure Probability: 9.31%

Event		Probability		LogNorm Parm		LogNorm Dist		
		Median	90%	m	s	Mode	Mean	Std.Dev.
Entry, Descent, and Landing Failure							**9.3E-2**	**2.1E-2**
1 Entry							**1.33E-2**	**4.8E-3**
	1.1 Cruise stage sep.	5.0E-4	1.0E-3	-7.60E+0	5.41E-1	3.73E-4	5.79E-4	3.37E-4
	1.2 Guidance error.	1.0E-3	2.0E-3	-6.91E+0	5.41E-1	7.46E-4	1.16E-3	6.75E-4
	1.3 Thermal protection.	5.0E-3	1.0E-2	-5.30E+0	5.41E-1	3.73E-3	5.79E-3	3.37E-3
	1.4 Parachute deploy.	5.0E-3	1.0E-2	-5.30E+0	5.41E-1	3.73E-3	5.79E-3	3.37E-3
2 Descent							**4.93E-2**	**1.86E-2**
	2.1 Heatshield separate.	1.0E-3	2.0E-3	-6.91E+0	5.41E-1	7.46E-4	1.16E-3	6.75E-4
	2.2 Bridle deploy.	5.0E-3	1.0E-2	-5.30E+0	5.41E-1	3.73E-3	5.79E-3	3.37E-3
	2.3 Altimeter operate.	5.0E-3	1.0E-2	-5.30E+0	5.41E-1	3.73E-3	5.79E-3	3.37E-3
	2.4 Airbag inflation.	1.0E-2	3.0E-2	-4.61E+0	8.57E-1	4.80E-3	1.44E-2	1.50E-2
	2.5 Retro-rocket burn.	1.0E-2	2.0E-2	-4.61E+0	5.41E-1	7.46E-3	1.16E-2	6.75E-3
	2.6 Bridle cut.	1.0E-2	2.0E-2	-4.61E+0	5.41E-1	7.46E-3	1.16E-2	6.75E-3
3 Landing							**2.76E-2**	**8.28E-3**
	3.1 Surface impact.	1.0E-2	2.0E-2	-4.61E+0	5.41E-1	7.46E-3	1.16E-2	6.75E-3
	3.2 Airbag retraction.	5.0E-3	1.0E-2	-5.30E+0	5.41E-1	3.73E-3	5.79E-3	3.37E-3
	3.3 Petal deploy.	1.0E-2	1.5E-2	-4.61E+0	3.16E-1	9.05E-3	1.05E-2	3.41E-3
4	AIM Flight Computer	5.0E-3	1.0E-2	-5.30E+0	5.41E-1	3.73E-3	**5.79E-3**	**3.37E-3**

Mars Pathfinder PDF



Stardust Spacecraft

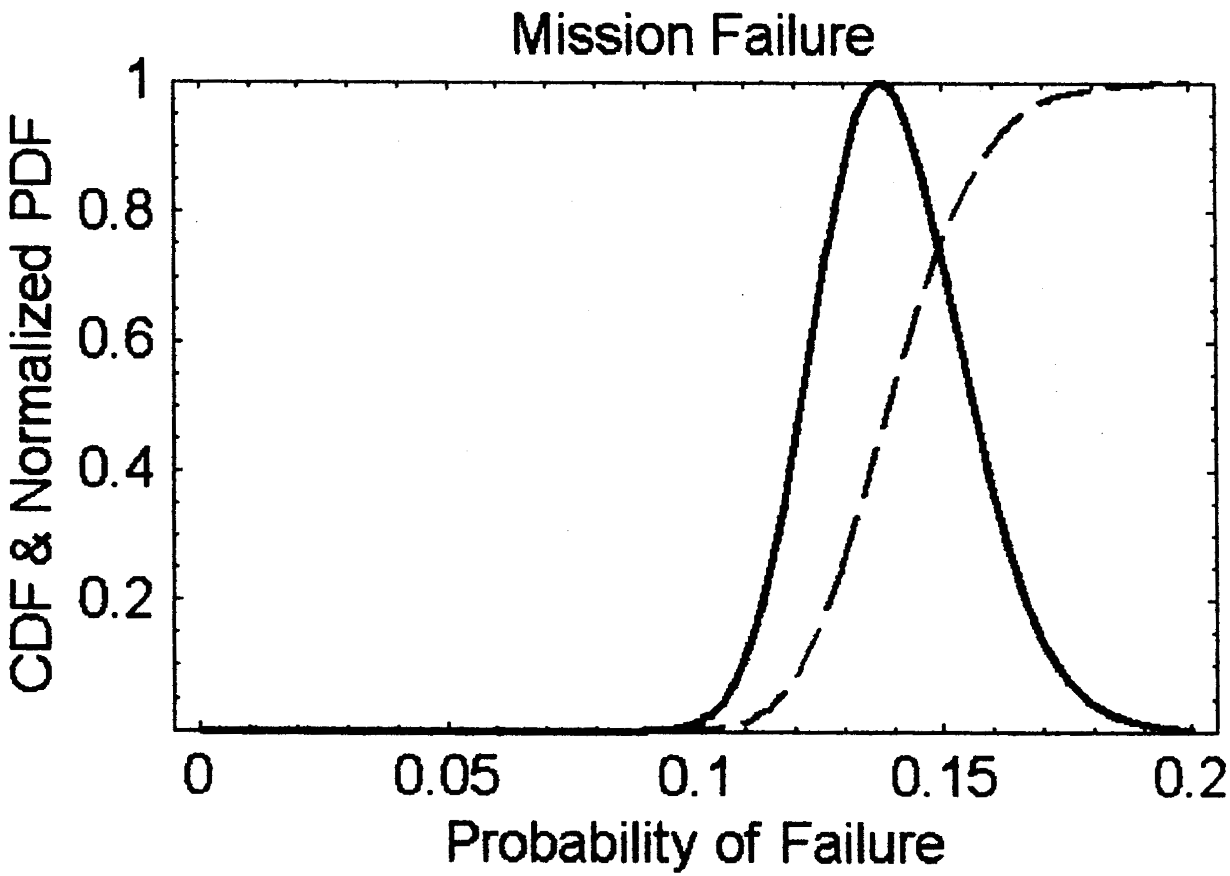
Stardust Risk Assessment

- Assessment from Launch Vehicle Separation to recovery of Science Capsule in Utah desert.
- All events in series---no redundancy modeled.
- Mission Modeled as series elements in MS Excel.
- Monte-Carlo simulation in JPL Excel Add-In.
- Training sessions for all probability assessors.
- Probabilities elicited from cognizant engineers.
- Project engineer reassessed probability of failure at mission level.
- Results not formally presented by Project.
- PRA done too late in development to influence design.
- Design conservatism obscured true risk.

Prototype Stardust Fault Tree

Event	Probability Distribution 50%	90%	Type	Mean	StdDev	Monte Carlo Mean
General						**2.295E-02**
S/C Structure (w/Whipple shield)	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Aerogel performance	Not Credible Failure			0.000E+00	0.000E+00	0.000E+00
Propulsion (despin, TCM, jets)	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Fuel Loading for entire mission	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
SRC Retention/Release	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Launch						**1.164E-02**
Launch vehicle injection	Not considered			0.000E+00	0.000E+00	0.000E+00
Launch vehicle separation	Not considered			0.000E+00	0.000E+00	0.000E+00
ACS Despin	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Solar Array Retention/Deployment	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Cruise						**5.640E-02**
SRC deployment & retraction	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Battery Operation	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Star Cameras	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Telecom Performance	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Thermal performance	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
IMU & Accelerometer	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
ACS S/W in C&DH	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
C&DH Hardware	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
C&DH Software	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Power	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Comet Encounter						**1.164E-02**
C&DH - no reset or swap	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
ACS performance with impacts	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Flyby trajectory	Not credible failure			0.000E+00	0.000E+00	0.000E+00
Collect 1,000 particles	Not credible failure			0.000E+00	0.000E+00	0.000E+00
Earth Return Phase						**4.638E-02**
SRC Structure	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Aeroshell aerodynamics	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
SRC Avionics (w/o battery)	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
SRC Battery	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Parachute	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
UHF Beacon	Not Credible Failure			0.000E+00	0.000E+00	0.000E+00
Heatshield/TPS performance	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
SRC Vent	Not Credible Failure			5.788E-03	3.374E-03	0.000E+00
Aerogel Canister Filter	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Entry Trajectory	5.00E-03	1.00E-02	TLognormal	5.788E-03	3.374E-03	5.788E-03
Stardust Failure Probability:						**1.401E-01**

Prototype Stardust Mission PDF



MBA* Criteria

1. Experts are poor processors of information.
2. Effective techniques for reducing overconfidence.
3. Decompose the problem.
4. Aggregate multiple experts.
5. Use structured group processes.
6. Combine expert judgments using math methods.

* A. Mosleh, Vicki M. Bier, and G. Apostolakis, *Methods for the Elicitation and Use of Expert Opinion in Risk Assessment: Phase 1 -- A Critical Evaluation and Directions for Future Research,* NUREG/CR-4962 and PLG-0533, Pickard, Lowe and Garrick, Inc., Prepared for the U.S. Nuclear Regulatory Commission, August 1987.

Critique of Process

- ❑ Done too late to influence design.
- ❑ Management and engineering biases present.
- ❑ Engineers don't understand statistical processes.
- ❑ Reluctance to accept subjective probabilities.
- ❑ Reluctance to accept PRA in general.

For Future Research

- New methodology and new culture needed for control of biases.
- Is a probability of a probability a probability? *
- Display PDF to expert.
  - CDF yields little feedback.
  - Fitting standard PDF to elicited CDF yields some feedback.
  - Need differentiable CDF.
    - » With strong monotonicity for unimodal PDF.
- Relation between knowledge and PDF.
  - Perhaps information theory has something to contribute.

* Brian Skyrms, "Higher Order Degrees of Belief," in *Prospects for Pragmatism, Essays In Honor of F. P. Ramsey*, D. H. Mellor (Ed.), Cambridge University Press, Cambridge, pp. 109-137, 1980.

Probability Elicitation References

- ❑ MBA: Mosleh, Bier, and Apostolakis.
  - "Methods for the Elicitation and Use . . . In Risk Assessment"
    - » NUREG/CR-4962 & PLG-0533, August 1987.
- ❑ Hoffman, Hora, et al.
  - "A Guide for Uncertainty Analysis . . ."
    - » NCRP Comm. #14, 10 May 1996.
- ❑ Stanford/SRI/SDG/Stael von Holstein.
- ❑ Literature.
  - Von Winterfeldt and Edwards.
  - Morgan and Henrion
  - Risk Analysis, Management Science, Plenum Press, JASA, Psychology, Nuclear Engineering, NRC, IEEE.